REMARKS

This Amendment is filed in response to the Office Action mailed on January 12, 2006. All objections and rejections are respectfully traversed.

Claims 6-11, 13-17, 20, 23, and 26-28 are pending in the case.

Claims 26-28 are added to better claim the invention.

Claim Rejections -35 U.S.C. §102

At paragraphs 4-5 of the Office Action, claims 6-11, 13-17, 20, 23 were rejected under 35 U.S.C. §102 as being anticipated by Eckstein et al., titled "Using Samba", published Nov. 1999, hereinafter Eckstein.

The present invention, as set forth in representative claim 6, comprises in part:

> 6. A method for creating and maintaining a plurality of virtual servers within a server, the method comprising the steps of:
> partitioning resources of the server to establish an instance of each virtual server by allocating units of storage and network addresses of network interfaces of the server to each instance of the virtual server, and sharing an operating system and a file system of the server among all of the virtual servers;
> ***enabling controlled access to the resources using logical boundary checks and security interpretations of those resources within the server***; and
> providing a vfiler context structure including information pertaining to a security domain of the vfiler.

By way of background, Eckstein discloses a system for setting up server configurations in Unix or Windows by describing the Samba server process replication system.

A server can be set up with guest use, printing share, specific volume for sharing, and read only and writeable capabilities. Problems with the Samba system are set out in Applicant's present specification at page 5, lines 3-10, as follows:

> "In an environment having multiple independent servers used to accommodate multiple security domains, all shares (and share names) must be distinct. However, if those servers are consolidated onto a single platform (by way of server process replication, such as Samba, or server bundling) using alias names for the server, the server names of the UNC paths to the shares may require change, since all share resources would be visible when accessed via any of the alias server names. In other words, although each server may have its own set of shares, users may have to change the UNC path definitions of those shares in order to access their data. "

In fact, Eckstein requires a user to enter a password to access private files, this is shown for example at page 99, which follows:

> "Note that users can still connect to the share using a valid username/password combination. If successful, they will hold the access rights granted by their own account and not the guest account. If a user attempts to log in and fails, however, he or she will default to the access rights of the guest account. You can mandate that every user who attaches to the share will be using the guest account (and will have the permissions of the guest) by setting the option guest only = yes."

Applicant respectfully urges that Eckstein does not disclose Applicant's claimed novel step of ***enabling controlled access to the resources using logical boundary checks and security interpretations of those resources within the server***. In further detail, ***boundary checks*** are performed by the file system of the storage operating system to verify that a current vfiler executing on the filer is allowed to access certain storage resources for a requested file stored on the platform. The ***boundary checks*** are based on configuration information, such as the unit of storage (qtree or volume) associated with

the file, acquired from an inode of the requested file. Specifically, a file system identifier and qtree identifier are validated in accordance with a multi-stage verification procedure to ensure that they are members of the storage resources allocated to the current vfiler. For every request to access a unit of storage, the ***boundary checks*** are performed using these identifiers to determine whether the requesting vfiler is authorized to access the storage resource. If the check reveals that the vfiler is not authorized to access the requested storage resource, the request is immediately denied. Otherwise, the request is allowed and the file system generates operations to process the request.. In contrast, Eckstein does not describe using ***boundary checks***.

Eckstein requires a user to enter a password or change a UNC paths. In contrast, Applicant's invention allows the operating system to check if a filer is allowed to access a particular vfiler.

Accordingly, Applicant respectfully urges that the Eckstein publication is legally precluded from anticipating the claimed invention under 35 U.S.C. § 102 because of the absence from the Eckstein publication of Applicant's step of ***enabling controlled access to the resources using logical boundary checks and security interpretations of those resources within the server***.

In the event that the Examiner deems personal contact desirable in disposition of this case, the Examiner is encouraged to call the undersigned attorney at (617) 951-3067.

All independent claims are believed to be in condition for allowance.

All dependent claims are believed to be dependent from allowable independent claims.

The Applicant respectfully solicits favorable action.

Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,

Shannen C. Delaney
Reg. No. 51,605
CESARI AND MCKENNA, LLP
88 Black Falcon Avenue
Boston, MA 02210-2414
(617) 951-2500